UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/927,928	08/09/2001	Rodric C. Fan	TRMB-2096	6041

70409 7590 01/05/2010

TRIMBLE NAVIGATION LIMITED C/O WAGNER BLECHER
123 WESTRIDGE DRIVE
WATSONVILLE, CA 95076

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
01/05/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/927,928	FAN ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 October 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6,8-11,15-17,20,25-27 and 29-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6,8-11,15-17,20,25-27 and 29-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application.
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 22, 2009 has been entered.

Claims 5, 7, 12-14, 18-19, 21-24, and 28 remain cancelled.

Claims 1, 6, 10, and 29 are amended.

Claims 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 are pending and herein considered.

Response to Arguments

Applicant's arguments and amendments with respect to the rejection(s) of claim(s) 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 under 35 USC 103a have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of United States Patent No. 6,055,314 to Spies et al.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-4, 6, 9-11, 16-17, 20, 26-27, 29-33 and 35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Each of Applicant's independent claims call for "transmitting the encrypted first key ***separate from*** the encrypted data packet to a wireline device ***in a first transmission***" or an equivalent thereof. The Examiner is unsure how it is that Applicant can transmit both the encrypted first key and the encrypted data packet "in a first transmission" and yet transmit the encrypted first key "separate from" the encrypted data packet.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4, 6, 9-11, 16-17, 20, 26-27, 29-33 and 35 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent No. 6,055,314 to Spies et al.

As per **claim 1**, Spies teaches a method for transmitting secured data over a wireless link, the method comprising:

utilizing a first key ("program key") to encrypt a payload (col.5 lines 10-24);

adding a header to the encrypted payload to form a data packet (col.9 lines 40-60);

utilizing a second key to encrypt the first key (col.5 lines 35-53);

utilizing a third key to encrypt the data packet (col.9 lines 40-60));

transmitting the encrypted first key separate from the encrypted data packet to a wireline device in a first transmission from a wireless device, wherein the wireline device decrypts the encrypted first key (col.3 lines 5-35; col.5 lines 35-53; col.8 lines 26-41); and

transmitting only the encrypted data packet without said first key over a wireless link to a gateway in a second transmission from the wireless device, wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the wireline device over an open network (col.3 lines 36-50); and

utilizing the wireline device and the first key from the first transmission to decrypt the encrypted payload (col.10 lines 49-56).

As per **claim 2**, Spies teaches wherein the first key comprises a symmetric key (col.6 line 59 thru col.7 line 67; col.10 lines 57-67).

As per **claim 3**, Spies teaches transmitting the encrypted first key to the wireline device, wherein the wireline device decrypts the encrypted first key using a private key associated with the second key (col.6 line 59 thru col.7 line 67; col.10 lines 57-67).

As per **claim 4**, Spies teaches wherein the third key comprises a symmetric session key (col.6 line 59 thru col.7 line 67; col.10 lines 57-67).

As per **claim 6**, Spies teaches a device for transmitting secured data over a wireless link, the device comprising:

an encryption engine which generates a first key, encrypts a payload according to the first key (col.5 lines 10-24), adds a header to the encrypted payload to form a data packet (col.9 lines 40-60), encrypts the first key according to a second key (col.5 lines 35-53) and encrypts the data packet according to a third key (col.9 lines 40-60); and

a wireless transceiver coupled to the encryption engine, the wireless transceiver transmitting the encrypted first key separate from the encrypted data packet to a server

in a first transmission from the device (col.3 lines 5-35; col.5 lines 35-53; col.8 lines 26-41) and transmitting only the encrypted data packet without said first key over the wireless link to a gateway in a second transmission from the device, wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the server over an open network (col.3 lines 36-50);

wherein the server decrypts the encrypted first key received in the first transmission and decrypts the encrypted payload of the second transmission using the decrypted first key (col.10 lines 49-56).

As per **claim 8**, Spies teaches wherein the first key employs a symmetric key (col.6 line 59 thru col.7 line 67; col.10 lines 57-67)

As per **claim 9**, Spies teaches wherein the payload comprises GPS location information obtained by the device and regarding a geographical location of the device (col.11 lines 40-60).

As per **claim 10**, Spies teaches a method for secured communication between a mobile device and a server on a wide area network, the method comprising:

encrypting a payload at the device using a first session key (col.5 lines 10-24);

encrypting the first session key at the mobile device using a public key (col.5 lines 35-53);

transmitting the encrypted first session key separate from the an encrypted data packet to the server over a link in a first transmission from the mobile device (col.3 lines 5-35; col.5 lines 35-53; col.8 lines 26-41);

decrypting the encrypted first session key at the server (col.10 lines 49-56);

adding a header to the encrypted payload to form a data packet at the mobile device (col.9 lines 40-60);

encrypting the data packet according to a second session key configured for secured communications over the wireless link (col.9 lines 40-60); and

transmitting only the encrypted data packet without said first key in a second transmission from the mobile device to a gateway which decrypts the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the server (col.3 lines 36-50);

wherein the server utilizes the decrypted first session key, decrypted from the first transmission to decrypt the encrypted payload (col.10 lines 49-56).

As per **claim 11**, Spies teaches wherein the decrypting the encrypted first session key at the server further comprises:
decrypting the encrypted first session key at the server using a private key associated with the public key (col.7-col.8).

As per **claim 15**, Spies teaches wherein the payload includes GPS location information obtained by the mobile device and associated with a geographical location of the mobile device (col.11 lines 40-60).

As per **claim 16**, Spies teaches generating the first session key at the device based on a random number (col.7-col.8; col.10).

As per **claim 17,** Spies teaches wherein the encrypting the payload at the device using the first session key further comprises encrypting the payload at the device using the first session key, wherein the first session key employs an encryption algorithm selected from a group of the encryption algorithms consisting of DESX and DES (col.7 lines 41-55).

As per **claim 20**, Spies teaches implementing an encryption algorithm selected from a group of encryption algorithms consisting of DESX and DES (col.7 lines 41-55).

As per **claim 25**, Spies teaches wherein the payload includes GPS location information obtained by the wireless device and associated with a geographical location of the wireless device (col.11 lines 40-60).

As per **claim 26**, Spies teaches utilizing a random number to generate the first key (col.7-col.8; col.10).

As per **claim 27**, Spies teaches a memory coupled to the encryption engine, wherein the memory stores the second key, and wherein the encryption engine accesses the second key from the memory (col.10).

As per **claim 29**, Spies teaches a computer readable storage medium, comprising program instruction for performing a method comprising:

encrypting a payload according to a first key (col.5 lines 10-24);

adding a header to the encrypted payload to form a data packet (col.9 lines 40-60);

encrypting the first key according to a second key (col.5 lines 35-53);

encrypting the data packet according to a third key configured for secured communications over a wireless link (col.9 lines 40-60);

transmitting the encrypted first key separate from the encrypted data packet to a server in a first transmission from a mobile device (col.3 lines 5-35; col.5 lines 35-53; col.8 lines 26-41); and

transmitting only the encrypted data packet without said first key over the link to a gateway in a second transmission from the mobile device (col.3 lines 36-50), wherein the gateway decrypts the encrypted data packet to recreate the encrypted payload and the header and forwards the encrypted payload and the header to the server and wherein the server decrypts the encrypted first key received in the first transmission and decrypts the encrypted payload using the decrypted first key (col.10 lines 49-56).

As per **claim 30**, Spies teaches wherein the first key comprises a symmetric key (col.6 line 59 thru col.7 line 67; col.10 lines 57-67; col.15 lines 43-57).

As per **claim 31**, Spies teaches

receiving the data packet at the gateway (col.8 lines 44-57);

decrypting the data packet at the gateway according to the third key (col.8 lines 44-57);

forwarding the encrypted payload to the server and receiving the encrypted first key at the server (col.15 lines 43-57);

decrypting the encrypted first key using a fourth key and decrypting the payload according to the decrypted first key (col.12 line 61 thru col.13 line 8; col.15 lines 43-57).

As per **claim 32**, Spies teaches wherein the first session key comprises a symmetric session key (col.6 line 59 thru col.7 line 67; col.10 lines 57-67; col.15 lines 43-57).

As per **claim 33,** Spies teaches implementing an encryption algorithm selected from a group of encryption algorithms consisting of DESX and DES (col.7 lines 41-55)).

As per **claim 34**, Spies teaches wherein the data packet includes GPS location information obtained by the mobile device and associated with a geographical location of the mobile device (col.11 lines 40-60).

As per **claim 35**, Spies teaches wherein the symmetric session key is generated based on a random number (col.7-col.8; col.10).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437